

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF VERMONT

SECURITIES AND EXCHANGE
COMMISSION,

Plaintiff,

v.

CHAD C. MCGINNIS, SERGEY
PUGACH, AND JANUSZ SUCHOWIEJKO

Defendants, and

BELLA PUGACH,

Relief Defendant.

Civil Action No. 5:14-CV-6

JULY 3, 2017 SUPPLEMENTAL EXPERT REPORT OF DANIEL L. REGARD II

I. INTRODUCTION

I am a Managing Director of Intelligent Discovery Solutions, Inc. (“iDiscovery Solutions”), an expert services and consulting firm that provides independent expert testimony and analysis, original authoritative studies, and strategic consulting services to the business and legal community.

I provide my opinions with a reasonable degree of professional certainty, based on information available to me at this time, and I reserve the right to modify these opinions if more information is provided.

I am being compensated at the hourly rate of \$500. The hourly rates of the iDiscovery Solutions professionals who have performed work at my direction in connection with my preparation of this report range from \$265 to \$500. My compensation is unaffected by the content of this report or my testimony or the outcome in this matter.

I previously submitted a report in this matter in which I opined upon regarding:

1. Mr. McGinnis' broad access to the Keurig Green Mountain¹ ("KGM") network as a result of his knowledge of a domain administrator account;
2. Mr. McGinnis' access of confidential business information ("CBI") folders on multiple occasions that would not have been accessible directly from his personally assigned corporate account, and;
3. Mr. McGinnis' subsequent copy of CBI files to non-company owned external USB connected devices in a manner consistent with an objective to limit detectability.
4. I identified one of those devices as a Western Digital USB device ("WD 2500BMV External USB Device", serial number 57442D575833304137394133393630).
5. I found that this USB device had been attached to two KGM computers identified as GMCR36152² and CHADMCLT³
6. In my first supplemental report, I found that this same USB device was previously attached to Mr. McGinnis' personal computer, DELLXPS-PC.

¹ Referred to as GMCR in my earlier report.

² This is a HP Compaq DC7700 Desktop computer assigned to Mr. McGinnis during his employment with KGM.

³ This is a HP EliteBook Laptop computer assigned to Mr. McGinnis during his employment with KGM.

In the time since my initial report on November 17, 2014, there have been major and minor improvements to the forensic tools I use. My use of these tools and my understanding of various artifacts on various operating systems have, accordingly, improved as well. By way of example, X-Ways has had two major upgrades to Version 18 (December 2014), and Version 19 (July 2016). EnCase has been upgraded to Version 8 (May 2016). Magnet IEF has been upgraded to Version 6.5 (November 2014); Version 6.6 (April 2015); Version 6.7 (September 2015); Version 6.8 (September 2016); and now Version 6.9. TZWorks is constantly releasing new “build packages” such as November 2016, March 2017, March 2017 (again), and May 2017.

I applied these newer tools in a supplemental analysis of Mr. McGinnis’ work-assigned laptop, CHADMCLT. In doing so, I identified previously undetected evidence of his use of the BATCHOPS user account, and previously undetected evidence of access to CBI on that same work-assigned laptop, as well as access to likely CBI on an unnamed work-assigned laptop that he used prior to CHADMCLT. Based on this supplemental analysis, I have reached the following conclusions:

1. The BATCHOPS domain account was found on the CHADMCLT laptop as the default user name for remote access to five different KGM computers.
2. Files that matched the names of known KGM CBI were stored on the laptop identified as CHADMCLT used by Mr. McGinnis starting in November 2011.
3. Files that matched the names of known KGM CBI were renamed and subsequently deleted from the CHADMCLT laptop.

4. Preview images (or “thumbnails”) of KGM PowerPoint presentations with titles of “Q3 2012 Performance”, “June 2012 BOD Financial Update”, and “Sept 2012 BOD Financial Update” were stored in the CHADMC user profile on the CHADMCLT laptop.
5. CHADMCLT contained traces of a laptop assigned to Mr. McGinnis prior to November 2011, CHADMCW7T. Those traces contain file names that match the naming style of known KGM CBI.

II. VARIOUS COMPUTERS

There are various computers referred to in this report, as well as my prior reports.

Here is summary of those computers and the reference names for each:

Name	Model	System Detail	
CHADMCLT	HP EliteBook Laptop	OPERATING SYSTEM: OS INSTALL DATE: USER PROFILE: CHADMC FIRST USE: CHADMC LAST USE: Description:	Windows 7 Enterprise 11/11/2011 11:29:56 -5 CHADMC 11/21/2011 09:15:15 -5 07/29/2013 14:26:42 -4 Laptop used by Mr. McGinnis between Nov 21, 2011 and the time of his termination on July 29, 2013.
CHADMCDT	HP Compaq 8200 Elite Workstation	OPERATING SYSTEM: OS INSTALL DATE: USER PROFILE: CHADMC FIRST USE: CHADMC LAST USE: USER PROFILE: BATCHOPS FIRST USE: BATCHOPS LAST USE: Description:	Windows 7 Enterprise 12/08/2011 21:08:03 -5 CHADMC 12/13/2011 10:11:00 -5 07/29/2013 18:38:26 -4 BATCHOPS 01/02/2013 09:19:24 -5 05/20/2013 11:25:20 -4 Workstation used by Mr. McGinnis between Dec 13, 2011 and the time of his termination on July 29, 2013

GMCR36152	HP Compaq DC 7700	OPERATING SYSTEM: OS INSTALL DATE: USER PROFILE: BATCHOPS FIRST USE: BATCHOPS LAST USE: Description:	Windows XP 01/11/2007 05:59:04 -5 BATCHOPS 07/16/2007 10:43:31 -4 07/12/2013 11:01:34 -4 Workstation used by Mr. McGinnis and was located in Mr. McGinnis' cube at the time of his termination in July 2013
CHADMCW7T	UNKOWN	UNKOWN	Windows computer used by Mr. McGinnis prior to Nov 21, 2011. Used as the source of files and user settings migrated to new CHADMCLT laptop.
DELLXPS-PC	Dell XPS	OPERATING SYSTEM: OS INSTALL DATE: USER PROFILE: FIRST USE: LAST USE: Description:	Windows 7 Professional 01/15/2012 18:49:11 -5 DELL XPS 01/15/2012 18:49:18 -5 09/04/2013 10:27:13 -4 Mr. McGinnis' personal computer. Forensic image was redacted prior to it being produced.

III. SOFTWARE USED FOR ANALYSIS

For my analysis, I relied on the following forensic software:

- 1) X-Ways Forensics v19.2 SR-3 x64
- 2) Internet Evidence Finder (IEF) v 6.9.0.5983
- 3) TZWorks v 2017.05.04.win64
- 4) EnCase Forensic v8.04

IV. FINDINGS

I performed a forensics analysis of the laptop used by Mr. McGinnis between November 21, 2011 and the time of this departure from KGM on July 29, 2013. The laptop was an HP EliteBook 2560p laptop and it was running the Windows 7 Enterprise operating.

The current Operating System was installed on the laptop on November 11, 2011 and on November 21, 2011, Mr. McGinnis' user profile named "CHADMC" was migrated to the new laptop from a previous Windows operating system and the computer name was changed from "GMCR72884" to "CHADMCLT". During the migration of this user profile to this laptop ("CHADMCLT"), evidence that files matching the names of known CBI had been stored and accessed using the preceding computer ("CHADMCW7T") was recorded in the migration log file.

V. THE MIGRATION OF DATA TO MR. MCGINNIS' NEW LAPTOP

The Microsoft User State Migration Tool ("USMT") is software created by Microsoft that is designed to facilitate moving a user's files and settings from one system to another. Generally, this is done when replacing a computer, but it can also be used to "refresh" an existing computer when the operating system is upgraded or reinstalled. The USMT uses a multi-step process to migrate data from one Windows installation to another.

The process consists of the following steps:

1. Scan the source computer and identify the files and user settings that will be migrated to the destination computer,
2. Copy the identified files and user settings from the source computer to an intermediate storage location, and
3. Copy the files and user settings from the intermediate storage location to the new destination computer.

First, the source laptop is scanned using the USMT “ScanState” tool. This is done to determine which files and settings will be migrated to the new computer. The specific files and settings that are migrated depend on the rules defined in the USMT configuration files.⁴ The ScanState tool will then copy the files and user settings that meet the criteria and save them in the “Migration Store,” a special file that stores the data to be migrated. The Migration Store is then used to migrate the user’s files and settings to the destination computer using the USMT “LoadState” tool.

Both ScanState and LoadState create logs of the actions taken when they are executed. Generally, the ScanState log is stored on the source computer and the LoadState log is stored on the destination computer. A LoadState log was found on CHADMCLT at the following location: C:\Logs\Chadmc\Chadmc-LoadState.log. I reviewed this LoadState log and found detailed information describing the content and settings of the original source computer at the time the USMT LoadState was run on it.

The source of the migration was a computer named “CHADMCW7T” which included a user profile named CHADMC. This computer was a member of the “WTBY” domain, and the user account that was active when the USMT ScanState was run was “CHADMC.”

⁴ The USMT uses XML configuration files to define the rules for the migration. These configuration files are stored in the USMT folder “C:\USMT\” on the CHADMCLT laptop. An evaluation of the USMT “Chadmc-LoadState.log” file shows that the following configuration files were used: miguser.xml, migapp.xml, pst.xml, exclusions.xml, and config.xml.

LoadState Log – Line 2236

...%COMPUTERNAME% <-> CHADMCW7T

LoadState Log – Lines 2335 & 2336

...%USERDOMAIN% <-> WTBY

...%USERNAME% <-> Chadmc

The migration occurred on November 21, 2011 and the source Migration Store was located on a shared folder at: \\laptops\laptops\Chadmc\USMT\USMT.MIG. At that time, and from this Migration Store, the CHADMC profile was migrated to the HP EliteBook laptop. This information was recorded in the log file at the following locations:

LoadState Log - Line 1 – Date and Time of Migration

...USMT Started at 2011/11/21:09:19:47.576 EST

LoadState Log - Line 277 – Migration Store

...Opening compressed store \\laptops\laptops\Chadmc\USMT\USMT.MIG

LoadState Log - Line 55 – Profile CHADMC Migrated

...Processing profile: C:\Users\Chadmc

VI. EVIDENCE OF CBI STORAGE AND ACCESS ON MCGINNIS' PRIOR LAPTOP

When migrating files and user settings to a new destination computer, the default configuration of the USMT process will exclude shortcuts files or “LNK” files that point to a file or “target” that is no longer in the expected location.⁵ As described on page 31 of my

⁵ The specific configuration instruction that will ignore LNK files for which the target is no longer in the expected location is named “IgnoreIrrelevantLinks”.

November 17, 2014 report, the Windows operating system uses LNK files to provide a shortcut or quick way of navigating to a specific file, folder, or application. When user data files are opened on a Windows computer, a LNK file is automatically created in the user's "Recent" folder.⁶ Each LNK file contains information including the location of the target file so that it can be found when the LNK file is used – hence its ability to act as a shortcut. During the migration process, however, if the target of a given LNK file is missing, there is no need to copy the LNK file to the destination computer. However, the LNK file, itself, may be logged for migration even though it is ultimately not migrated.

This happened during the migration of the CHADMC profile to CHADMCLT. Specifically, the LoadState log recorded details, including the file name and location of target files which were no longer found in the expected location. Of the LNK files that were not migrated, three had target with files names similar to or that followed the naming convention of known CBI. The three specific LNK files and target files include:

Verbal remarks 4QFY11 Draft 1.5.doc

1. LoadState Log – Line 20623 – LNK File
C:\Users\Chadmc\AppData\Roaming\Microsoft\Office\Recent\Verbal remarks 4QFY11 Draft 1.5.LNK
 2. LoadState Log – Line 20625 – Target of LNK File
...Src LNK target: C:\Users\Chadmc\Desktop\Verbal remarks 4QFY11 Draft 1.5.doc
-

⁶ Each user profile on a computer maintains a unique folder of LNK files to recently used target files and folders at the following location: %USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\.

3. Similar files names⁷ from the KGM
\\Money\apps\FINANCE\Private\IR\FY2011\Q2\Drafts\ folder:
Verbal Remarks Q2'11 Draft 1.2
Verbal Remarks Q2'11 Draft 1.3
Verbal Remarks Q2'11 Draft 1.4
Verbal Remarks Q2'11 Draft 1.5
Verbal Remarks Q2'11 Draft 1.6
Verbal Remarks Q2'11 Draft 1.7
Verbal Remarks Q2'11 Draft 1.7.CLEAN

Prepared remarks 4QFY11 Draft 1.5.doc

1. LoadState Log – Line 20546 – LNK FILE
C:\Users\Chadmc\AppData\Roaming\Microsoft\Office\Recent\Prepared remarks
4QFY11 Draft 1.5.LNK
2. LoadState Log – Line 20548 – Target of LNK File
...Src LNK target: C:\Users\Chadmc\Desktop\Prepared remarks 4QFY11 Draft 1.5.doc
3. Similar files names⁸ from KGM
\\Money\apps\FINANCE\Private\IR\FY2011\Q2\Drafts\ folder:
Prep remarks 2QFY11 Draft 1.2
Prep remarks 2QFY11 Draft 1.3
Prep remarks 2QFY11 Draft 1.3-accepted...
Prep remarks 2QFY11 Draft 1.4
Prep remarks 2QFY11 Draft 1.5
Prep remarks 2QFY11 Draft 1.6
Prep remarks 2QFY11 Draft 1.7
Prep remarks 2QFY11 Draft 1.7.CLEAN

⁷ Plaintiffs Exhibit 18 page “GMCR MC00001516” includes screen captures of the files stored on the server in the following protected location where CBI was maintained: \\MONEY\APPS\FINANCE\PRIVATE

⁸ Plaintiffs Exhibit 18 page “GMCR MC00001516” includes screen captures of the files stored on the server in the following protected location where CBI was maintained: \\MONEY\APPS\FINANCE\PRIVATE

Unanimous Written Consent - Comp Comm Nov 11 2011.doc

1. LoadState Log – Line 20614 – LNK File
C:\Users\Chadmc\AppData\Roaming\Microsoft\Office\Recent\Unanimous Written Consent - Comp Comm Nov 11 2011.LNK
2. LoadState Log – Line 20616 – Target of LNK File
...Src LNK target: C:\Users\Chadmc\Desktop\Unanimous Written Consent - Comp Comm Nov 11 2011.doc
3. Similar folder names⁹ from KGM \\Money\apps\BOD\OFFICIAL MINUTES\ folder:
 \2013 - FEB 15 Action for Unanimous Written Consent (CSR)\
 \2013 - MAR 25 Action for Unanimous Written Consent (BOD)\
 \2013 - MAR 25 Action for Unanimous Written Consent (COMP)\
 \2013 - MAY 20 Action for Unanimous Written Consent (GOV)\
 \2013 - MAY 24 Action for Unanimous Written Consent (GOV)\
 \2013 - MAY 3 Action for Unanimous Written Consent (BOD)\
 \2013 May 17 Action for Unanimous Written Consent (GOV)\
 \2013 May 20 Action for Unanimous Written Consent (GOV)\

In summary, the entries in the USMT LoadState log file show that CBI documents named “Prepared Remarks 4QFY211 Draft 1.5.doc”, “Verbal remarks 4QFY11 Draft 1.5.doc”, and “Unanimous Written Consent - Comp Comm Nov 11 2011.doc” were:

A) Saved in the desktop folder on CHADMCW7T,

⁹ Evidence of the “Unanimous Written Consent” folders is described in pages 21 – 29 of my November 17, 2014 report and further detailed in “Exhibit H - CBI Folders Accessed.xlsx”. These folder names were browsed using GMCR36512 workstation and the evidence was extracted from the ShellBAG registry values stored in the WTBX\BATCHOPS user profile.

B) The files were opened at while stored in the desktop folder, creating LNK files, but

C) The files did not reside in the same location with the same file names when CHADMCW7T was migrated to CHADMCLT.

If the LNK files had not been present on the prior computer, they would not exist in the Migration Store. And if the Target files were not present on the prior computer, the LNK files pointing to them would not exist.

VII. EVIDENCE OF CBI FILES BEING RENAMED AND DELETED FROM CHADMCLT

Additional evidence of KGM CBI being stored on CHADMCLT (the laptop assigned to Mr. McGinnis) was found in the file system change journal on that computer. The change journal stores information or transactional details about the folders and files stored on a Windows computer. The change journal is stored in a hidden file named \$UsnJrnl and is a feature that has been enabled by default starting with the Windows Vista operating system in January 2007.¹⁰ The change journal maintains a log of transactions including the creation, modification, renaming, and deletion of files and folders. I examined the CHADMCLT change journal and found multiple files with a similar file name to files identified by KGM as

¹⁰ The NTFS change journal is stored in the alternate data stream of a hidden file located at “\$Extend\$UsnJrnl:\$J”. My analysis included a review of the live \$UsnJrnl, previous copies of the change journal from Windows volume shadow copies (“VSS”), as well as recovered fragments of previously existing entries in the change journal. I used both X-Ways Forensics and the TZWorks Windows Journal Parser to examine the journal entries.

CBI. I also found two files with exact file names to files produced by KGM from the protected folders they used to maintain CBI. Below are the details of the two files:

Bizwire Cheat Sheet.doc

1. A file named Bizwire Cheat Sheet.doc was stored on the CHADMCLT laptop
2. The file was deleted on May 2, 2012 at 14:16:47 UTC
3. A file with that exact name was stored on KGM H:\ drive at the following location: \\money\apps\PR\RELEASES\Bizwire Cheat Sheet.doc
4. A file named Bizwire Cheat Sheet.doc was produced by KGM with the bates number "GMCR MC00053848"
5. The file named Bizwire Cheat Sheet.doc that was produced by KGM included the username, password, and instructions on how to log into and submit press releases to the http://connect.businesswire.com website

Non-GAAP tables.xls

1. A file named Non-GAAP tables.xls was stored on the CHADMCLT laptop at the following location: C:\Users\Chadmc\Desktop\Pre 7-13\docs\Non-GAAP tables.xls
2. The file name was changed to tables.xls on Sept 17, 2012 at 14:03:26 UTC
3. The file was deleted to the recycle bin 11 seconds later at 14:03:37 UTC
4. The recycle bin was emptied 40 seconds later at 14:04:17 UTC
5. A file with that exact name was stored on KGM H:\ drive at the following location:
\\money\apps\FINANCE\Private\Quarterly\Q2_2012\Non-GAAP tables.xls
6. A file named Non-GAAP tables.xls was produced by KGM with the bates number "GMCR MC00050323"

In addition to the two files with exact file name matches, the change journal from the CHADMCLT laptop included information about six files with names similar to those produced by KGM from protected CBI storage locations. All 6 of these additional files were deleted at the same time as “Bizwire Cheat Sheet.doc” on May 2, 2012 at 14:16:47 AM UTC, the of the KGM announcement of Q2FY12 earnings in a press release titled “Green Mountain Coffee Roasters, Inc. Reports Second Quarter Fiscal 2012 Results”.

GMCR 2012 Annual Meeting Draft 1.1.ppt
BOD March 12 Keurig Board Update - v4 Tab 5.6.doc
BOD SCBU Update 3-14-12 Tab 5.5.doc
BOSE Comm Plan 1 0.docx
Project Seesaw and BOSE SG Level 1 Sept 13 2011.ppt
Revised Keurig SCBU BOI 2012 PR Plan 2 9 12.ppt

Taken as a whole, the existence of these 8 files in the change journal located on the CHADMCLT laptop used by Mr. McGinnis evidences that files with the names of KGM CBI were stored on the laptop and they were subsequently deleted. Of the 8 files, 7 of the deletions occurred on the day of a major earnings announcement: May 2, 2012.

VIII. THUMBNAILED OF CBI STORED ON CHADMCLT

The Windows operating system takes many actions to speed up or improve the user experience. Many of these actions include “caching.” Caching is the process by which commonly used data is stored in an easily accessed format in an easily accessed location to

facilitate future use. Caching is used for Internet access, the creation of LNK files, computer chip performance, hard drive retrieval, and in many, many other areas.

One of the areas where Windows uses caching to speed performance is when presenting a small preview or “thumbnail” for files in Windows Explorer (“Explorer”). When browsing a file folder in Explorer, a user can opt for Explorer to display thumbnail previews of the files rather file listings. In such a configuration, a digital photograph would show a reduced size image of the photo, a MS Word Document would show an image of the first page of the document, and a PowerPoint Presentation would show the first slide. However, the process of creating a thumbnail preview takes time. For this reason, and in order to make subsequent viewings go faster, Windows will keep, or “cache”, the thumbnails in a special file called the “thumbcache_*.db.”¹¹ This is significant because even after the source document has been deleted, a thumbnail image may still reside in the thumbcache and can provide insight into the content of the now-deleted file.

¹¹ The thumbcache files are located under the user’s profile at the following location: %USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer\. The system maintains multiple thumbcache_*.db files, one for each resolution of thumbnail stored. The “*” in “thumbcache_*.db” is substituted with the size of thumbnails, each containing difference resolutions of thumbnails. The files are named “thumbcache_32.db”, “thumbcache_96.db”, “thumbcache_256.db”, etc.

IX. THE THUMBNAIL CACHE ON THE CHADMCLT LAPTOP

The thumbnail cache is stored by Windows in the user's profile. For the CHADMCLT laptop I reviewed the thumbcache file located under the CHADMC profile.¹²

This file is stored under the following file path:

\\Users\\Chadmc\\AppData\\Local\\Microsoft\\Windows\\Explorer\\thumbcache_256.db

In reviewing the images within the cache file, I identified the thumbnail images below that represent files containing CBI:



Figure "June 2012 BOD Financial Update"



"HIGHLY CONFIDENTIAL – INTERNAL USE ONLY"

¹² The thumbcache_*.db files were reviewed and extracted using the X-Ways Forensics v.19.2 software.



Figure "Q3 2012 Performance"



Figure "Sept 2012 BOD Financial Update"

Each of these images shows what appears to be the first slide of a PowerPoint presentation. The titles of the presentations imply that the content is financial in nature and

when looking closely, at the bottom right of the two “BOD Financial Update” thumbnails is text, that while blurred in the thumbnail, reads “HIGHLY CONFIDENTIAL – INTERNAL USE ONLY.”

The presence of these thumbnails on CHADMCLT under the CHADMC profile is evidence that the original files they represent were at some time browsed by the CHADMC user account. Without this activity, Windows would not have created the Thumbnails in the first place, or added them to the cache. The original files are not present on the computer, but the Thumbnail Cache continues to provide evidence that the files were browsed at one time.

X. MCGINNIS’ KNOWLEDGE OF THE “BATCHOPS” ADMINISTRATIVE ACCOUNT

Mr. McGinnis had knowledge of the BATCHOPS username and password at least as early as January 27, 2007 when Michael Yaeger sent Chad McGinnis the BATCHOPS username and password in an email.¹³ Below is the excerpt from the January 2007 email:

-----Original Message-----

From: Michael Yaeger <Michael.Yaeger@gmcr.com>

To: Chad McGinnis <Chad.McGinnis@gmcr.com>; Nate Isham <Nate.Isham@gmcr.com>

Sent: Sat Jan 27 10:19:48 2007

Subject: RE: ilo

All the iLO's use the username "Batchops" and the password is [REDACTED] Note that the username is case sensitive. More problems with Dove?

Mike

¹³ Deposition of Mr. Chad McGinnis on October 15, 2014. Exhibit 35.

In addition to the email received by McGinnis, the BATCHOPS username and password was found in a deleted contact card (“VCF”) that was once saved in Mr. McGinnis’ GMCR mailbox. The contact card was attached to an email with the subject of “FW: Server Logins - Application Servers (SCM & HR Production) [GMCR]” and sent by Carleen Costey <Carleen.Costey@gmcr.com> to Chad McGinnis <Chad.McGinnis@gmcr.com> on March 24, 2010.

In my initial report, I identified knowledge of BATCHOPS repeated in 2008, and 2011; evidence of BATCHOPS on GMCR36152 in 2007, 2009, and from January 2013 through July 2013; and evidence of BATCHOPS on CHADMCDT in early 2013. Now, I have found evidence of BATCHOPS on CHADMCLT in 2012 and early 2013, as detailed below.

XI. MCGINNIS’ USE OF THE “BATCHOPS” ADMINISTRATIVE ACCOUNT

The Windows operating system includes a feature called remote desktop connection or “RDP” to enable users to access or log into a remote computer using a local network or even over the internet.¹⁴ This convenient feature allows computer users to remotely access a computer using a full graphical interface with similar functionality to sitting down in front of

¹⁴ The Windows remote desktop connection uses a network protocol called the “Remote Desktop Protocol”. As a result, the common acronym for a remote desktop connection is “RDP”. Historically, the remote desktop was called terminal services and remote desktop client executable is named “mstsc.exe”.

the computer and logging in to it directly. To remotely connect to a Windows computer, the user opens a software application called the Remote Desktop Connection¹⁵ or they can simply type in “MSTSC” in a RUN or CMD prompt. Once the Remote Desktop Connection or “RDP Client” is opened, the user needs to provide at the computer name or address, the user name, and a password¹⁶.

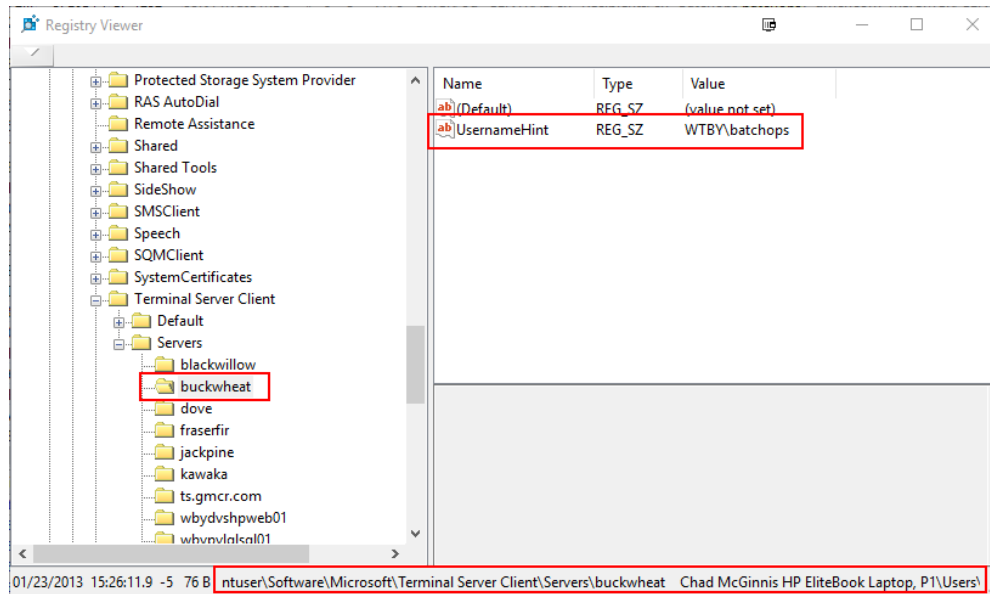
For convenience, Windows maintains the last username used for each remote desktop connection. The next time the user remotely connects to a computer, the username is automatically filled out. The server name, the user name, and the date and time of the first connection¹⁷ to a remote computer can be determined by examining a Windows user registry file called the NTUSER.dat. The details about the user name are stored in registry key called the “UsernameHint”. I examined the NTUSER.dat file that was dedicated to Mr. McGinnis’ user profile on the CHADMCLT laptop and found that he had logged into five different computers using the BATCHOPS administrative user account. The following is a screen capture of Mr. McGinnis’ NTUSER.dat registry file from the CHADMCLT laptop that

¹⁵ The Remote Desktop Connection application is actually a shortcut or LNK file that points to the “mstsc.exe”. The files are located at “C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Remote Desktop Connection.lnk” and “C:\Windows\System32\mstsc.exe” respectively.

¹⁶ The remote desktop client includes a number of configuration options that can be saved in a “.rdp” file.

¹⁷ The UsernameHint registry key records the first time the specific username is used to access a remote server. If a new username is used, the UsernameHint is updated along with the date the key was modified.

details the login information, including the saved WTBY\batchops user account for the GMCR computer named “buckwheat”.



This information extracted from the computer used by Mr. McGinnis shows the following:

1. The user logged into the CHADMCLT laptop using the WTBY\CHADMC user account accessed a server named “buckwheat”
2. The access occurred on at least January 23, 2013 at 15:26:11 UTC
3. The access was made using the WTBY\batchops user account

The following is a chart which details the five different servers that were accessed using the WTBY\batchops domain user account:

Server:	dove
LastWriteTime:	02/23/2012 13:32:52.102 UTC
UsernameHint:	WTBY\batchops

Server:	wbypvlgweb01
LastWriteTime:	04/11/2012 12:15:07.958 UTC
UsernameHint:	WTBY\batchops

Server:	wbypvlgsql01
LastWriteTime:	04/11/2012 12:40:05.274 UTC
UsernameHint:	WTBY\batchops

Server:	Wbypvocapp01
LastWriteTime:	06/11/2012 15:56:34.533 UTC
UsernameHint:	WTBY\batchops

Server:	buckwheat
LastWriteTime:	01/23/2013 20:26:11.927 UTC
UsernameHint:	WTBY\batchops

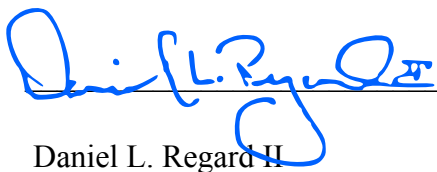
Figure "RDP Servers with BATCHOPS User Hint"

XII. SUMMARY

My previous reports revealed that Mr. McGinnis had availed himself of access to KGM identified confidential business information ("CBI") throughout 2013.

My further analysis of CHADMCLT and traces of its predecessor, CHADMCW7T, has now revealed that Mr. McGinnis also availed himself of access to KGM CBI in late 2011 and at various times during 2012, and demonstrated usage of BATCHOPS during 2012 and early 2013.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on July 3, 2017 in Rehobeth Beach, DE.



Daniel L. Regard II

July 3, 2017

Date